

AMENDMENTS TO THE CLAIMS:

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1-6. (Canceled)

7. (New) A gate device with a connection for connecting to a local network and a connection for an external network, wherein the external network is located outside the local network domain, wherein the connection provides at least one communication channel between the local network and the external network, wherein the gate device is located in the at least one communication channel and configured to

(a) perform a file-selective check for access possibilities to a file outside the local network by checking the file sent from the local network to the connection for presence of a security tag before the file is sent to the external network via the at least one communication channel, and

(b) block the sending of the file to the external network if the security tag is found to be present in the file.

8. (New) A method for protecting information transport from a local network domain of communicating computers to an external network located outside the local network domain, wherein at least one communication channel connects the local network domain and the external network, the method comprising the steps of:

providing a security tag in a file accessible by the communicating computers;
coupling a gate device to the local network domain and the external network, wherein the gate device is located in the at least one communication channel and between the local network domain and the external network;

performing a file-selective check for access possibilities to the file outside the local network domain via the gate device checking the file sent from the local network domain for presence of a security tag before the file is sent to the external network via the at least one communication channel, and

blocking the sending of the file to the external network if the security tag is found to be present in the file.

9. (New) A computer system, comprising:

a local network domain of communicating computers, wherein the communicating computers are configured to access a file;

a first connection for communication with an external network, wherein the external network is located outside the local network domain of communicating computers, wherein the first connection provides at least one communication channel between the local network domain and the external network; and

a first gate device is located in the at least one communication channel and coupled between the local network domain and the external network, wherein the first gate device is configured to

- (a) perform a file-selective check for access possibilities to the file outside the local network domain by checking the file sent from the local network domain to the first connection for presence of a security tag before the file is sent to the external network via the at least one communication channel, and
- (b) block the sending of the file to the external network if the security tag is found to be present in the file.

10. (New) The computer system according to claim 9, further comprising:

one or more second gate devices coupled between the local network domain and the external network, wherein the one or more second gate devices are located

within the at least one or more communication channels and configured to

(a) perform file-selective checks for access possibilities to files outside the local network domain by checking the files sent from the local network domain for the presence of security tags before sending the files to the external network via the one or more communication channels, and

(b) block the sending of the files if the security tags are found to be present in the files.

11. (New) The computer system according to claim 9, further comprising:
an encrypted file automatically generated by the gate device if the security tag is found to be present in the file.

12. (New) The computer system according to claim 11, wherein the gate device is configured to send the encrypted file to the external network via the at least one communication channel.

13. (New) The computer system according to claim 9, further comprising:
anti-tamper code combinable with the security tag to prevent removal of the security tag from the file.

14. (New) The computer system according to claim 9, wherein each of the communicating computers is configured to apply the security tag to the file.

15. (New) The computer system according to claim 9,
an encrypted file or an encrypted portion of a file generated by a communicating computer when the communicating computer applies the security tag to the file.

16. (New) The computer system according to claim 9, further comprising
a memory means for storing data located within the gate device, wherein the
gate device is configured to store data regarding presence of the security tag and/or
sending of the file in a log file in the memory.
17. (New) The computer system according to claim 9, further comprising:
a tag detector located within the gate device, wherein the tag detector is
configured to examine the file for presence of the security tag.
18. (New) A gate device with a connection for connecting to a local network and a
connection for an external network, wherein the external network is located outside the
local network domain, wherein the connection provides at least one communication
channel between the local network and the external network, wherein the gate device is
located in the at least one communication channel and configured to
- (a) perform a file-selective check for access possibilities to a file outside the
local network by checking the file sent from the local network to the connection for
presence of a security tag before the file is sent to the external network via the at least
one communication channel, and
 - (b) send the file to the external network only if the security tag is found to be
present in the file.